Kaoru Uchida
Filed 2/5/01
Q62922
1 of 1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年 ２月 ３日

出願番号
Application Number: 特願２０００－０２５８１６

出願人
Applicant (s): 日本電気株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年１１月１０日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願
【整理番号】　33509686
【提出日】　平成12年 2月 3日
【あて先】　特許庁長官殿
【国際特許分類】　G06K 9/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　内田　薫
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100088812
　【弁理士】
　【氏名又は名称】　▲柳▼川　信
【手数料の表示】
　【予納台帳番号】　030982
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　バイオメトリクス入力装置及びバイオメトリクス照合装置

【特許請求の範囲】

【請求項１】　個人に固有の生体特徴であるバイオメトリクスをディジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でディジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵に基づいて暗号化して出力するバイオメトリクス暗号化手段とを有することを特徴とするバイオメトリクス入力装置。

【請求項２】　前記センサ手段と前記秘密情報保持手段及び前記バイオメトリクス暗号化手段とを不可分な部分として構成するようにしたことを特徴とする請求項１記載のバイオメトリクス入力装置。

【請求項３】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項１または請求項２記載のバイオメトリクス入力装置。

【請求項４】　個人に固有の生体特徴であるバイオメトリクスをディジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でディジタル化されたバイオメトリクスに前記秘密情報保持手段に保持された暗号化鍵を電子透かしとして埋め込む電子透かしエンコーダとを有することを特徴とするバイオメトリクス入力装置。

【請求項５】　前記センサ手段と前記秘密情報保持手段及び前記バイオメトリクス暗号化手段とを不可分な部分として構成するようにしたことを特徴とする請求項４記載のバイオメトリクス入力装置。

【請求項６】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項４または請求項５記載のバイオメトリクス入力装置。

【請求項７】　バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に前記保持手段に保持された前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段

とを有することを特徴とするバイオメトリクス照合装置。

【請求項８】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項７記載のバイオメトリクス照合装置。

【請求項９】　バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に別途入手した前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項１０】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項９記載のバイオメトリクス照合装置。

【請求項１１】　バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と前記保持手段に保持された暗号化鍵とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項１２】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項１１記載のバイオメトリクス照合装置。

【請求項１３】　バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と別途入手した前記バイオメトリクス入力装置固有の秘密情報とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項１４】　前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項１３記載のバイオメトリクス照合装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はバイオメトリクス入力装置及びバイオメトリクス照合装置に関し、特に情報セキュリティ等におけるユーザ確認、個人識別のためのバイオメトリクス入力装置及びバイオメトリクス照合装置に関する。

【０００２】

【従来の技術】

情報の電子化やネットワークを通じての情報サービスにおいて、データの盗聴・改竄や「なりすまし」といった不正・犯罪に対抗するセキュリティの確保のためには、情報にアクセスする人間が正当な権限を持つユーザであるか、または価値の交換の相手が自分の望むユーザであるかを確認するための本人確認の実現が必須の条件となる。

【０００３】

現在、本人確認には磁気カードやパスワードが利用されているが、例えばカードをなくしたり、パスワードを忘れてしまうと本人でも使えないという不便さがあるのはもちろん、いずれの場合も盗難・偽造や盗み見・推量によって容易に他人がなりすませるという問題点がある。

【０００４】

そこで、これらの問題点を解決するバイオメトリクスが用いられる。バイオメトリクスとは指紋のような個人に特有な生体特徴を利用するものである。人間の指先の皮膚紋様である指紋は「万人不同」・「終生不変」という特徴を持つとされ、表皮が損傷を受けてもその奥の不変な真皮から同じ指紋が復元されるため、精密な個人の同定を可能にするバイオメトリクスとして広く知られている。

【０００５】

バイオメトリクスによって個人を認証するシステムは基本的に、ユーザが提示したバイオメトリクスをシステム側で取得する「バイオメトリクス入力装置」と、入力されたデータを処理し照合に用いる特徴を求める「特徴抽出部」と、予め求めて記憶しておく正規ユーザについての登録データ（「テンプレート」）と、

登録データと入力データ（の特徴同士）とを比較して同一人物であるか否かを決定する「照合・判定部」とから構成されている。

【０００６】

照合の結果、特徴が十分類似し、バイオメトリクスの提示者が登録ユーザであると判定されれば、認証成功ということで、認証要求者は要求するサービスを受けられる。以下、バイオメトリクスの例として指紋を挙げて説明する。

【０００７】

指紋の入力装置としては従来、光学方式、特に高コントラストな画像を得るためにプリズムでの全反射を利用する方法のみが用いられてきている。これはＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）光源で発した光をプリズムに当ててからＣＣＤ（Ｃｈａｒｇｅ　Ｃｏｕｐｌｅｄ　Ｄｅｖｉｃｅ）のような受光素子で受け、プリズムの反射面に置いた指の凹凸を反射率の違いに反映させ、ディジタル画像化するというものである。

【０００８】

また近年は、光学方式以外のセンシングを可能とする素子として、半導体チップの表面に直接接触させた指紋からその凹凸をセンスする、例えば静電容量方式のもの、温度や電界の差を検知する方式のもの等も実用化されつつある。

【０００９】

【発明が解決しようとする課題】

指紋照合処理の実現方法としては、入力装置が指紋の入力だけを行い、識別処理が接続されたＰＣ（パーソナルコンピュータ）やネットワークで結ばれたサーバ等で行うという方法がとられることがある。

【００１０】

このように、指紋入力装置（スキャナ）と照合処理部とが分離している場合、入力装置（入力スキャナ、入力センサと呼ばれることもある）は指紋画像の入力を行い、それをケーブル等を通してＰＣに送り、そこで特徴抽出や照合・判定処理が実行される。

【００１１】

このような構成ではケーブルを付け替えて他の情報機器を結び、他の機会に入

手した他人の指紋の画像データを、入力センサを装って照合処理部に入力するというセキュリティアタックがあり得る。この場合、照合処理部ではサービスを要求する本人の指紋と考えてサービスを許可するが、実際には他人の指紋であったということが起こりうる。

【００１２】

そこで、本発明の目的は上記の問題点を解消し、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことができるバイオメトリクス入力装置及びバイオメトリクス照合装置を提供することにある。

【００１３】

【課題を解決するための手段】

本発明によるバイオメトリクス入力装置は、個人に固有の生体特徴であるバイオメトリクスをディジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でディジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵に基づいて暗号化して出力するバイオメトリクス暗号化手段とを備えている。

【００１４】

本発明による他のバイオメトリクス入力装置は、個人に固有の生体特徴であるバイオメトリクスをディジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でディジタル化されたバイオメトリクスに前記秘密情報保持手段に保持された暗号化鍵を電子透かしとして埋め込む電子透かしエンコーダとを備えている。

【００１５】

本発明によるバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に前記保持手段に保持された前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【００１６】

本発明による他のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に別途入手した前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【００１７】

本発明による別のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と前記保持手段に保持された暗号化鍵とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【００１８】

本発明によるさらに別のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と別途入手した前記バイオメトリクス入力装置固有の秘密情報とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【００１９】

すなわち、本発明のバイオメトリクス入力装置は、入力装置で取得されるバイオメトリクスデータを入力装置固有の鍵で暗号化し、あるいは入力装置固有のデータを電子透かしとして埋め込むことで、照合装置側でバイオメトリクス入力装置の正当性を確認可能とする。

【００２０】

これによって、バイオメトリクス入力装置が改造・置換され、あるいは出力信

号が置換された場合にそれを検知することが可能となるので、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことが可能となる。

【００２１】

【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例によるバイオメトリクス入力装置の構成を示すブロック図である。図１においてはＰＣ等においてユーザのログインを指紋で行う場合の構成の一例を示しており、指紋入力装置１をケーブル等のローカルな接続によってＰＣに接続し、ＰＣ上のソフトウェアで指紋照合部２が動作するようになっている。

【００２２】

指紋入力装置１には指紋センサ１１が装備されており、指紋センサ１１はユーザの指が接触した際にその指紋画像を撮影し、撮影した入力画像をディジタルデータに変換してから画像暗号化部１３に送る。暗号化鍵保持部１２は一般ユーザ等に知られていない秘密情報としてその指紋入力装置１の個体固有の暗号化鍵を保持する。これは、例えば２５６ビットのビット列等である。

【００２３】

画像暗号化部１３は暗号化鍵保持部１２からその暗号化鍵を受取り、これを鍵として入力画像の暗号化処理を行う。この暗号化処理としては、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓａｎｄａｒｄ）を例とするような共通秘密鍵方式の暗号化方法を用いることができるが、また一方、ＲＳＡ方式を例とするような公開鍵方式（非対称暗号系）の暗号化方式を利用することも可能である。この場合、指紋入力装置１の持つ秘密鍵を暗号化に用いることになる。

【００２４】

また、用途によっては複雑な暗号化処理でなくても、入力画像のラインや画素毎にシフトしたり、入れ替えたりするスクランブル処理を採用し、そのスクランブルを規定するルールを暗号化鍵として暗号化鍵保持部１２に置くという方法も可能である。

【００２５】

一方、指紋入力装置１の構成法としては、指紋センサ１１、画像暗号化部１３、暗号化鍵保持部１２を不可分な方法で構成することが望ましい。不可分であるとは、ここの部分の解読や改造を図る不当な第三者が、指紋センサ１１から画像暗号化部１３への内部信号、暗号化鍵保持部１２から画像暗号化部１３への内部信号を解読したり、それらの信号を外部からの信号で置き換えたり、あるいはそれぞれの構成要素の中身を解読したり改造したりできないように構成するということである。

【００２６】

この実現法としては、指紋センサ１１の画像取得及びディジタル化を実行する半導体チップと同一チップ上に画像暗号化部１３と暗号化鍵保持部１２とを焼き込むという方法が有効である。一例としては、指紋センサ１１の撮像部としてＣＭＯＳ（Ｃｏｍｐｌｅｍｅｎｔａｒｙ　Ｍｅｔａｌ　Ｏｘｉｄｅ　Ｓｅｍｉｃｏｎｄｕｃｔｏｒ）のイメージャチップを利用し、その同一チップ上で暗号鍵の保持から暗号化演算までを行い、暗号化した結果を出力信号とするという実装があり得る。

【００２７】

あるいは、指紋センサ１１の指紋画像取得方法として半導体センサによる静電容量方式の指紋センシングを利用し、その半導体センサ上に暗号鍵の保持から暗号化演算までを実装するということもできる。

【００２８】

指紋入力装置１とケーブル等のローカルな接続によって結ばれた指紋照合部２ではその内部の暗号化情報保持部２４に、その指紋照合部２が接続して使用する指紋入力装置１の個体毎に固有な暗号化鍵を、その入力装置の識別子（装置ＩＤ）と対にして記憶しておき、現在接続されているはずの指紋入力装置１の装置ＩＤに対応する鍵を指紋復号化部２１に渡す。画像復号化部２１はその鍵を用い、指紋入力装置１から受取った信号を復号する。

【００２９】

この復号処理は指紋入力装置１の画像暗号化部１３の処理内容に対応したものを用い、正しく意味ある信号が復元できることをもって、指紋入力装置１及びそ

こから送られてくる信号の正当性を確認することなる。

【００３０】

例えば、画像暗号化部１３が共通秘密鍵方式の暗号化方法を用いていれば、暗号化鍵保持部１２に保持されたものと同一の鍵を用いた復号を行い、これで正しく復号できる場合には指紋入力装置１及びそこから送られてくる信号が正当なものであることを確認することができる。

【００３１】

また、公開鍵方式（非対称暗号系）の暗号化方式であれば、指紋入力装置１の暗号化鍵保持部１２に保持された秘密鍵に対応する公開鍵を用いて復号する。これで正しく復号できる場合には指紋入力装置１及びそこから送られてくる信号が正当なものであることを確認することができる。

【００３２】

さらに、画像暗号化部１３が入力画像のラインや画素毎にシフトしたり、入れ替えたりするスクランブル処理を用いた場合にも、暗号化鍵保持部１２が持っているはずのスクランブルを規定するルールを鍵として暗号化情報保持部２４に保持しておき、それを用いて対応する復号化を行う。これで正しく復号できる場合には指紋入力装置１及びそこから送られてくる信号が正当なものであることを確認することができる。

【００３３】

指紋特徴抽出部２２は画像復号化部２１で復号された結果の画像情報から指紋照合に用いる特徴を計算する。ユーザ別指紋登録情報テーブル２６は指紋照合に用いる指紋特徴情報をユーザ毎に保持している。指紋特徴照合部２３は指紋特徴抽出部２２で求められた指紋特徴とユーザ別指紋登録情報テーブル２６に登録されているユーザの指紋特徴との照合を行い、結果を照合結果判定部２５に渡す。

【００３４】

以上の指紋センサ１１、指紋特徴出部２２、指紋特徴照合部２３を含む指紋照合装置の実現例としては、特開昭５６－２４６７５号公報や特開平４－３３０６５号公報に記載された「指紋照合装置」がある。

【００３５】

特開昭５６－２４６７５号公報に記載された「指紋照合装置」では、指紋等の照合に際して、指紋紋様を特徴付ける各特徴点の位置Ｘ，Ｙ及び方向Ｄとともに各特徴点により固有に決定される局所座標系を複数個の扇形領域に分割した近傍における最近傍点と上記特徴点との隆線数、すなわちリレーションを検査することによって、安定で、かつ精度の高い照合を可能にしている。

【００３６】

また、特開平４－３３０６５号公報に記載された「指紋照合装置」では、登録されている一つの指もしくは複数の指の全てと入力指紋との照合を行うことによって、暗証番号の盗難や忘却に関与しない、操作性が優れかつ信頼性の高い同定を可能としている。

【００３７】

照合結果判定部２５は指紋入力装置１から送られてくる信号の正当性と、指紋特徴照合部２３で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。先に述べたように、指紋照合部２は使用されているはずの指紋入力装置１に固有で秘密であるはずの鍵情報を暗号化情報保持部２４のテーブルから探索し、それを用いて指紋入力装置１から送られる信号を復号し、それが正しく意味ある信号であるか否かを確認する。

【００３８】

正しく意味ある信号とはすなわち、指紋入力装置１において指紋センサ１１から出力された信号の形式に合致していることを意味し、これが合致している場合には指紋入力装置１が正当なもので、また指紋入力装置１からの信号は途中で改変されていないことが確認できたとして、指紋照合結果は信頼できるものであると判断する。

【００３９】

一方、合致していない等、正しく復号できなかった場合には、それは指紋入力装置１が正当なものではないか、または指紋入力装置１からの信号が途中で改変されたことを意味するので、指紋照合結果は信頼できるものではないと判断することになる。

【００４０】

図２は本発明の他の実施例による画像入力装置の構成を示すブロック図である。図２においては本発明の一実施例と同様に、ＰＣ等においてユーザのログインを指紋で行う場合の構成の一例を示しており、指紋入力装置３をケーブル等のローカルな接続によってＰＣに接続し、ＰＣ上のソフトウェアで指紋照合部４が動作する。

【００４１】

指紋入力装置３には指紋センサ１１が装備されており、指紋センサ１１はユーザの指が接触した際にその指紋画像を撮影し、撮影した入力画像をディジタルデータに変換してから電子透かしエンコーダ３１に送る。指紋入力装置秘密情報保持部３３は一般ユーザ等に知られていない秘密情報としてその指紋入力装置３の個体固有の秘密情報を保持する。これは、例えばパスワードのような文字列等である。

【００４２】

電子透かしエンコーダ３１は指紋入力装置秘密情報保持部３３からその秘密情報を受取り、電子透かしエンコード方式によってこれを入力画像に埋め込む。電子透かし技術とは次のような特徴を持つ。

【００４３】

すなわち、（１）透かしデータをコンテンツの中に、不可視の状態で埋め込むことができる、（２）透かしを埋め込んだ者が必要な時に抽出することが可能である、（３）透かしはコンテンツを加工しても残り、抽出が可能である、（４）コンテンツの利用価値を保ったまま第三者が電子透かしを除去するのは困難であるという特徴を持つ。（２）は暗号化技術におけるキーのような情報を設定し、キーを用いなければ情報が取り出せないような仕組みを設けることによって行われる。

【００４４】

上記の電子透かし技術を使用することによって、コンテンツである指紋画像を劣化させることなく、電子透かしデータをその中に埋め込むことができ、そのデータを秘密に保つことができる。また、指紋画像を大幅に劣化させることなく、透かしデータを分離・削除・改変することもできない。電子透かし技術の実現法

の例としては、例えば特開平８－２４１４０３号公報に記載の方法や特開平１０－２２４７９３３号公報に記載の技術等がある。

【００４５】

特開平８－２４１４０３号公報に記載の方法では、ウォーターマーク画像の画素を検査し、その値が指定された「透明」値でない画素のそれぞれについて、現画像の対応する画素を、その色度ではなく輝度を変更することによって修正することで、画像の内容を明瞭に見ることができるが、画像の無認可使用をおもいとどまらせる可視のマークをもたらすようにしている。

【００４６】

また、特開平１０－２２４７９３３号公報に記載の技術では、電子透かしが挿入されたＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔａ　Ｇｒｏｕｐ）ストリームとともに、挿入された電子透かしデータも出力することで、挿入する電子透かしデータの管理を簡単にしている。

【００４７】

尚、上記の指紋入力装置３の構成法としては、本発明の一実施例と同様に、指紋センサ１１、指紋入力装置秘密情報保持部３３、電子透かしエンコーダ３１を不可分な方法で構成することが望ましい。また、電子透かしエンコーダ３１の出力信号はこのままユーザの指紋画像データが見える形で含むので、通信内容秘匿のために暗号部３２において暗号化処理を行う。これは通常よく使われるＤＥＳの秘密共通鍵方式等の暗号化方式でよく、以下に述べる復号部４１と鍵情報を共用していればよい。

【００４８】

指紋入力装置３とケーブル等のローカルな接続によって結ばれた指紋照合部４においては、まず復号部４１において通信内容秘匿のための暗号化を解き、電子透かしエンコーダ３１の出力信号を復元する。その後、電子透かしデコーダ４２において、電子透かしエンコーダ３１のエンコードの方法に対応したデコード（復号化）処理を行い、指紋画像信号からそこに埋め込まれた透かしデータを分離して検出する。

【００４９】

指紋入力装置３は指紋画像信号とは別に、その装置固有のＩＤ（識別子）を指紋照合部４に送る。指紋照合部４ではその内部の指紋入力装置ＩＤ保持部４３に、その指紋照合部４が接続して使用する指紋入力装置３の個体に対応する秘密情報をその入力装置の識別子（装置ＩＤ）と対にして記憶しておく。この秘密情報は該当指紋入力装置の指紋入力装置秘密情報保持部３３に保持されている情報と同一のものである。

【００５０】

指紋入力装置ＩＤ保持部４３は指紋入力装置３から受取ったＩＤでこのテーブルをひき、対応する秘密情報を読出して指紋入力装置ＩＤ比較部４４に渡す。指紋入力装置ＩＤ比較部４４はその値と、電子透かしデコーダ４２において検出された透かしデータとを比較する。もしも、指紋入力装置３が正当なものであればこれらは一致するはずであり、そうでなければ不一致となる。

【００５１】

指紋特徴抽出部２２は電子透かしデコーダ４２から出力された画像情報から指紋照合に用いる特徴を計算する。ユーザ別指紋登録情報テーブル２６は指紋照合に用いる指紋特徴情報をユーザ毎に保持しているものである。指紋特徴照合部２３は指紋特徴抽出部２２で求められた指紋特徴とユーザ別指紋登録情報テーブル２６に登録された指紋特徴との照合を行い、結果を照合結果判定部２５に渡す。

【００５２】

照合結果判定部２５は指紋入力装置ＩＤ比較部４４が判定する指紋入力装置３の正当性と、指紋特徴照合部２３で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。先に述べたように、指紋照合部４は使用されているはずの指紋入力装置３に固有で秘密であるはずの情報が電子透かしとして埋め込まれていれば、指紋入力装置３が正当なもので、また指紋入力装置３からの信号が途中で改変されていないことを確認することができたとして、指紋照合結果を信頼できるものであると判断する。

【００５３】

そうでない場合には、それは指紋入力装置３が正当なものではないか、または指紋入力装置３からの信号が途中で改変されたことを意味するので、指紋照合結

果を信頼できるものではないと判断することになる。

【００５４】

図３は本発明の別の実施例による画像入力装置の構成を示すブロック図である。図３においては本発明の他の実施例による画像入力装置をネットワークで結ばれた指紋照合に拡張したものである。

【００５５】

指紋入力装置５はユーザが利用するサービスクライアント７に接続されている。これは例えばユーザのオフィスの机の上にあるＰＣ、ユーザの家庭にあるＰＣ、あるいは店舗の店頭等にある公衆向けのＰＯＳ（Ｐｏｉｎｔ　Ｏｆ　Ｓａｌｅｓ）端末でもよい。これらのサービスクライアントは顧客であるユーザに対してさまざまな情報サービスや電子商取引の提供端末として働くが、ユーザの本人確認・認証に関しては指紋サーバ６と指紋入力装置５との通信を、中身を変えずに橋渡しする透明な仲介者として機能する。

【００５６】

サービスクライアント７に接続された指紋入力装置５は本発明の他の実施例と同様の構成を持ち、同様の動作を行う。電子透かしが埋め込まれた指紋入力画像はサービスクライアント７を通過して指紋サーバ６に送られる。

【００５７】

サービスクライアント７とネットワークによって結ばれた指紋サーバ６は基本的に本発明の他の実施例と同様の構成を持ち、同様の動作を行う。すなわち、電子透かしを検出し、これによって判定される指紋入力装置５の正当性と、指紋特徴照合部２３で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。

【００５８】

但し、指紋入力装置５は、本発明の他の実施例の場合と異なり、指紋画像信号とは別に指紋入力装置秘密情報保持部３３に保持された秘密情報を、公開鍵暗号部５１が指紋サーバ６に対応するＲＳＡ方式の公開鍵を用いて暗号化して指紋サーバ６に送る。

【００５９】

秘密鍵復号部６１では送られてきた信号を自分の公開鍵に対応した秘密鍵によって復号し、指紋入力装置ＩＤ比較部４４での比較に用いる。指紋サーバ６に対応するＲＳＡ方式の公開鍵を用いて暗号化された秘密情報は、その公開鍵に対応した秘密鍵によってのみ復号可能である。

【００６０】

この部分については本発明の他の実施例に準じて、ネットワーク内に結ばれた全ての指紋入力装置５に対応する秘密情報と指紋入力装置５との対を予め指紋サーバ６がその内部に保持しておくという実現法ももちろん可能ではあるが、指紋入力装置５の数が多くなり、また変更・交換等に対応するためには、このように別のチャネルで直接秘密情報を送る方が優れているといえる。

【００６１】

指紋サーバ６は照合結果判定部２５の出力をサービスクライアント７に知らせ、指紋を入力したユーザが正規のユーザでありかつ指紋入力装置５が正規の装置であると判定の結果から確認できた時に限り、サービスクライアント７はユーザの要求するサービスをそのユーザに対して提供する。

【００６２】

上記の本発明の実施例の説明では、バイオメトリクスの一例として指紋の場合を挙げて説明しているが、指紋センサ１１と、指紋特徴抽出部２２、指紋特徴照合部２３の部分を別のバイオメトリクスを入力し、特徴を抽出して照合する手段で置換すれば、掌紋、顔、虹彩、網膜血管パターン、掌形、筆跡、声紋等の他のバイオメトリクスを使用することも可能である。例えば、声紋の場合にはマイクで入力され、ディジタル化された後の音声データに対してマイクと不可分な装置で暗号化や電子透かしの埋め込みを施すことで、入力部の正当性を確認することができる。

【００６３】

このように、照合装置以外は解読できない信号、あるいはその中に埋め込まれた電子透かしを解読し、また改変できない信号をバイオメトリクス入力装置と照合装置との間での通信に用いることによって、バイオメトリクス入力装置が改造、置換されず正当なものであることを判定して本人認証を実行することができる

【００６４】

これによって、バイオメトリクス入力装置が照合装置とケーブルやネットワーク等で接続され、分離している場合でも、ケーブルを付け替えて他の情報機器を結び、他の機会に入手した他人の指紋の画像データを、入力センサを装って照合処理部に入力するという種類のセキュリティアタックを防ぐことができる。つまり、照合処理部ではサービスを要求する本人の指紋と考えてサービスを許可するが、実際は他人の指紋であったということは起こり得ない。

【００６５】

すなわち、データが登録されていない不適合スキャナからの指紋データで置き換えられた場合、データの一部に操作が加えられた場合、一部が失われた場合にはそれらを検知し、認証結果に反映させることができる。

【００６６】

また、本発明の別の実施例の構成をとることによって、ネットワーク上に多数のバイオメトリクス入力装置がある場合にも、それぞれが正当なものであることを確認しながらユーザ認証を実現することができる。

【００６７】

【発明の効果】

以上説明したように本発明によれば、個人に固有の生体特徴であるバイオメトリクスをディジタル化し、そのディジタル化したバイオメトリクスを予め設定された秘密情報である暗号化鍵に基づいて暗号化して出力することによって、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことができるという効果がある。

【図面の簡単な説明】

【図１】

本発明の一実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

【図２】

本発明の他の実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

【図３】

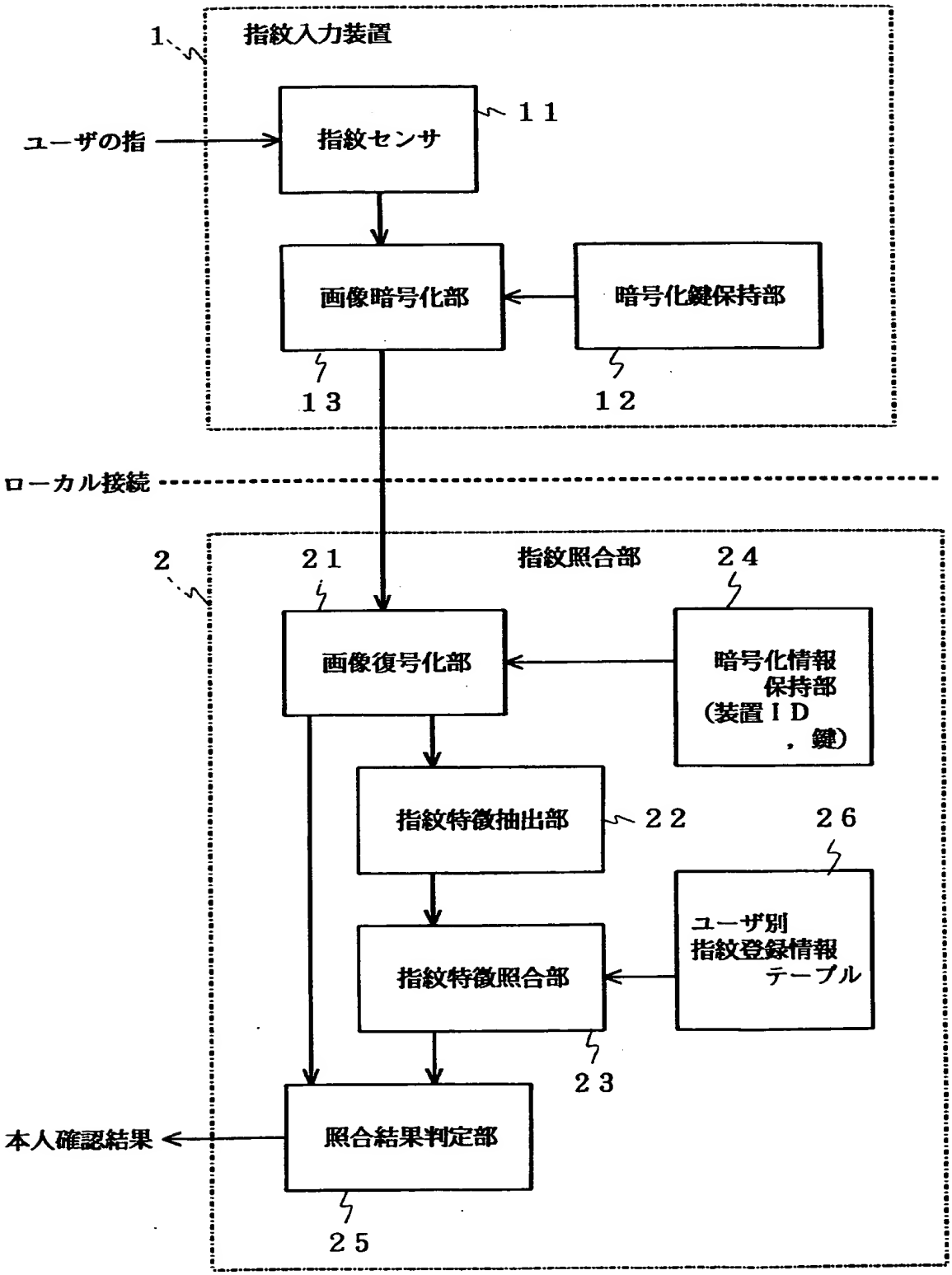
本発明の別の実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

【符号の説明】

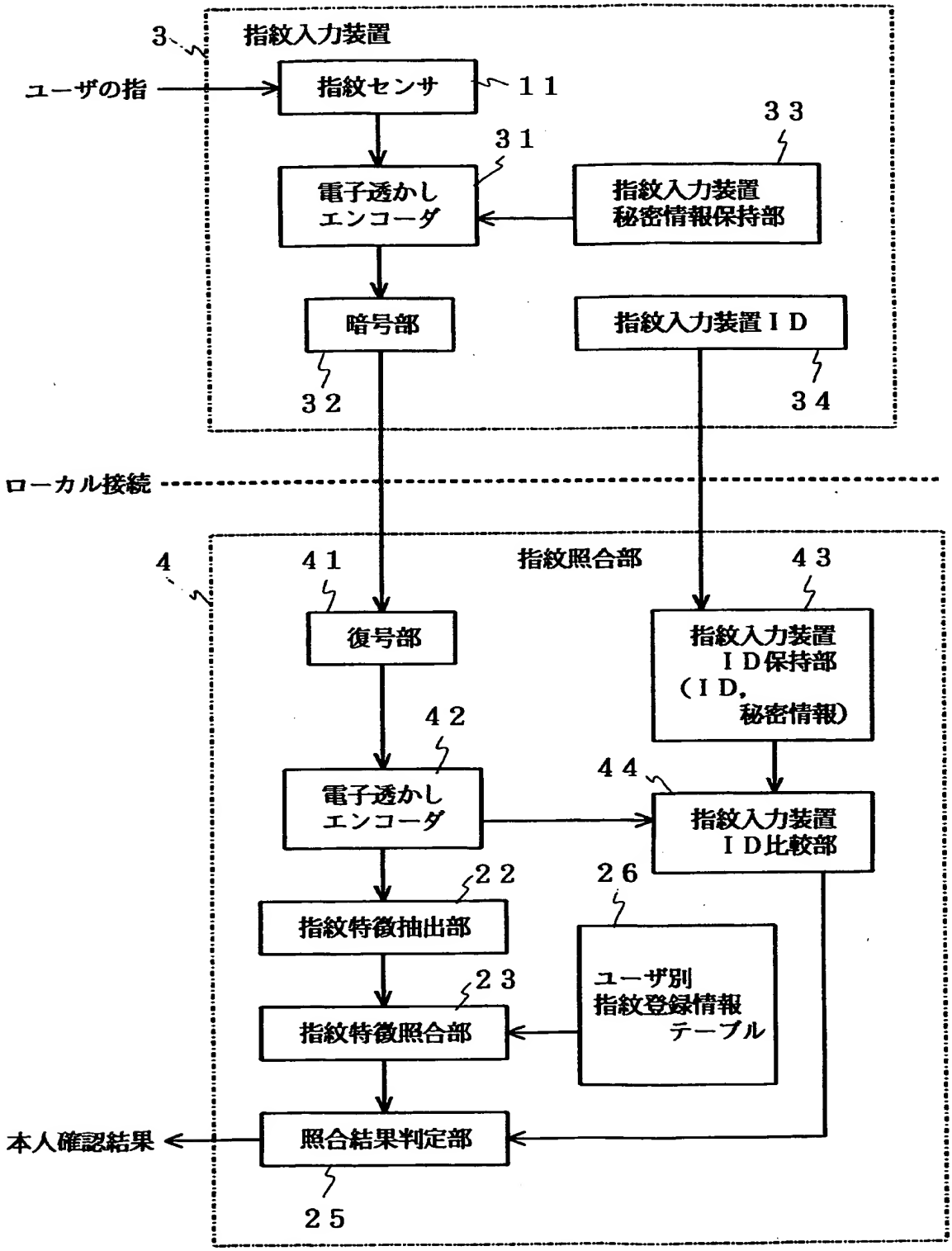
１，３，５　指紋入力装置
２，４　指紋照合部
６　指紋サーバ
７　サービスクライアント
１１　指紋センサ
１２　暗号化鍵保持部
１３　画像暗号化部
２１　画像復号化部
２２　指紋特徴抽出部
２３　指紋特徴照合部
２４　暗号化情報保持部
２５　照合結果判定部
２６　ユーザ別指紋登録情報テーブル
３１　電子透かしエンコーダ
３２　暗号部
３３　指紋入力装置秘密情報保持部
４１　復号部
４２　電子透かしデコーダ
４３　指紋入力装置ＩＤ保持部
４４　指紋入力装置ＩＤ比較部
５１　公開鍵暗号部
６１　秘密鍵復号部

【書類名】　図面

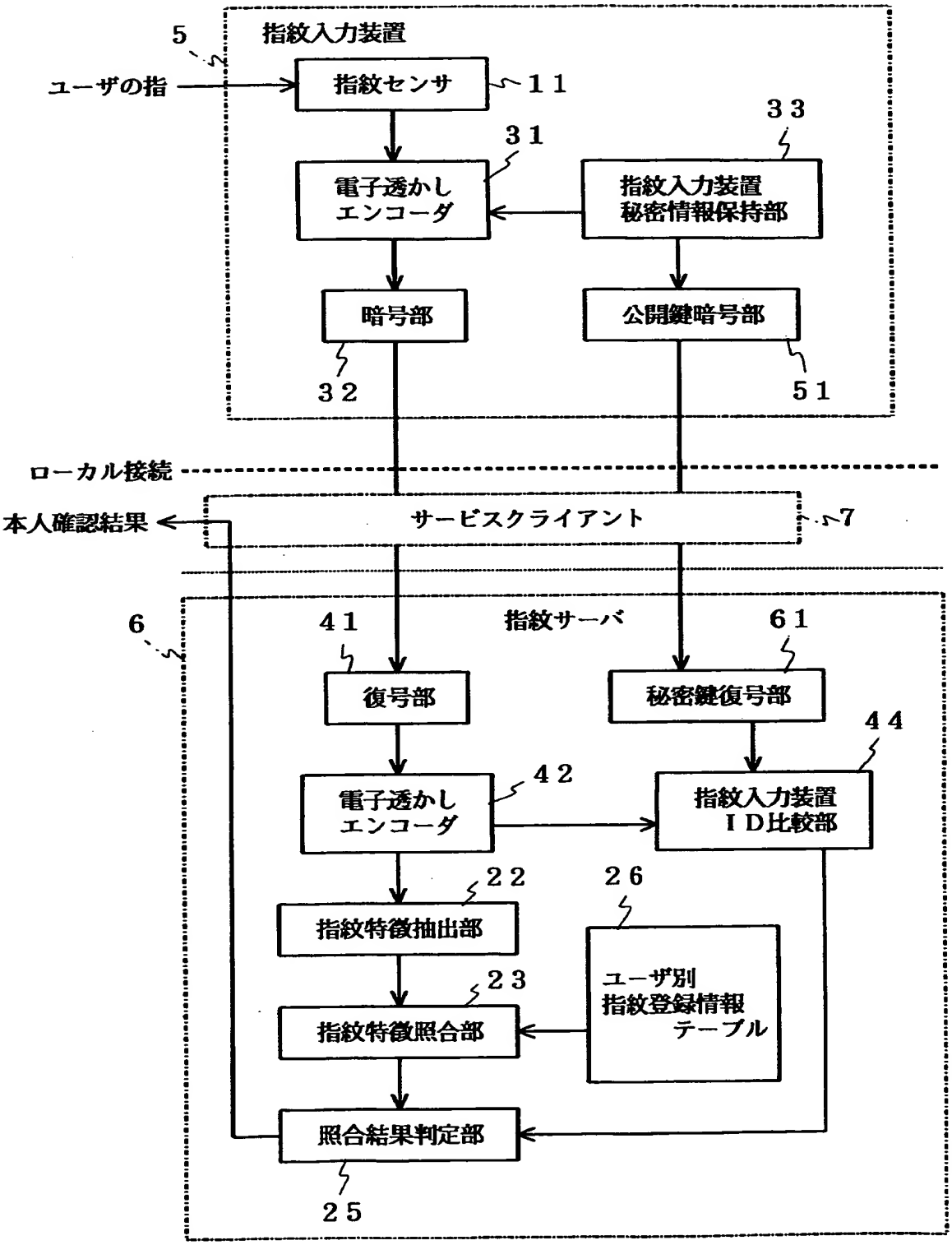
【図１】


1
指紋入力装置
ユーザの指
指紋センサ
１１
画像暗号化部
暗号化鍵保持部
１３
１２
ローカル接続
2
２１
指紋照合部
２４
画像復号化部
暗号化情報
保持部
(装置ＩＤ
，鍵)
指紋特徴抽出部
２２
２６
ユーザ別
指紋登録情報
テーブル
指紋特徴照合部
２３
本人確認結果
照合結果判定部
２５

【図２】


3
指紋入力装置
ユーザの指
指紋センサ
１１
３３
３１
電子透かし
エンコーダ
指紋入力装置
秘密情報保持部
暗号部
指紋入力装置ＩＤ
３２
３４
ローカル接続
4
４１
指紋照合部
４３
復号部
指紋入力装置
ＩＤ保持部
（ＩＤ，
秘密情報）
４２
４４
電子透かし
エンコーダ
指紋入力装置
ＩＤ比較部
２２
２６
指紋特徴抽出部
ユーザ別
指紋登録情報
テーブル
２３
指紋特徴照合部
本人確認結果
照合結果判定部
２５

【図３】


5
指紋入力装置
ユーザの指
指紋センサ
11
33
31
電子透かし
エンコーダ
指紋入力装置
秘密情報保持部
暗号部
公開鍵暗号部
32
51
ローカル接続
本人確認結果
サービスクライアント
7
6
41
指紋サーバ
61
復号部
秘密鍵復号部
44
42
電子透かし
エンコーダ
指紋入力装置
ＩＤ比較部
22
26
指紋特徴抽出部
ユーザ別
指紋登録情報
テーブル
23
指紋特徴照合部
照合結果判定部
25

【書類名】　　要約書

【要約】

【課題】　バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことが可能なバイオメトリクス入力装置を提供する。

【解決手段】　指紋センサ１１は指が接触した際にその指紋画像を撮影し、撮影した入力画像をディジタルデータに変換してから画像暗号化部１３に送る。画像暗号化部１３は暗号化鍵保持部１２から暗号化鍵を基に入力画像の暗号化処理を行う。画像復号化部２１は暗号化情報保持部２４からの鍵を用い、指紋入力装置１から受取った信号を復号する。指紋特徴抽出部２２は復号された結果の画像情報から指紋照合に用いる特徴を計算する。指紋特徴照合部２３は指紋特徴抽出部２２で求められた指紋特徴とユーザ別指紋登録情報テーブル２６に登録されているユーザの指紋特徴との照合を行い、結果を照合結果判定部２５に渡す。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社